UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,386,122 B1

APPLICATION NO.: 09/889918

DATED: June 10, 2008

INVENTOR(S): Louis Guillou et al.

hereby corrected as shown below:

It is certified that error appears in the above-identified patent and that said Letters Patent is

Page 1 of 2

Column 7

Line 54 delete " $r_i Q_{i1}^{d1}$ " and insert -- $r_i Q_{i1}^{d1}$ --.

Column 16

Line 46 delete " $D^{\nu}G_1^{d1}$ " and insert -- D^{ν}/G_1^{d1} --.

Column 24

Line 1 delete "mode" and insert -- mod --.

Line 10 delete "mode" and insert -- mod --.

Line 11 delete "mode" and insert -- mod --.

Column 27

Line 15 delete " $d - d_1$ " and insert -- $d = d_1$ --.

Column 28

Line 58 delete " $G_i^{d'}i$ " and insert -- G_i^{di} --.

Column 30

Line 43 delete " $G_1^{68_1d_1}$ " and insert -- $G_1^{6_1d_1}$ --.

Column 31

Line 10 delete " $Q_{1hu\ d}$ " and insert -- $Q_1^{d_1}$ --.

Line 11 delete " Qm^{d_m} " and insert -- $Q_m^{d_m}$ --.

Line 40 delete "Mis" and insert -- M is --.

Line 53 delete "F," and insert -- f, --.

Line 56 delete " $G_1^{\varepsilon_1 d_2}$ " and insert -- $G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2}$ --.

UNITED STATES PATENT AND TRADEMARK OFFICE CERTIFICATE OF CORRECTION

PATENT NO. : 7,386,122 B1 APPLICATION NO. : 09/889918

: June 10, 2008

INVENTOR(S)

DATED

: Louis Guillou et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 31 (Continued)

Line 61 delete " $0 \le d_i \le 2^k$ " and insert -- $0 \le d_i \le 2^k$ --.

Line 64 delete "on eor" and insert -- one or --.

Signed and Sealed this

Page 2 of 2

Twenty-third Day of September, 2008

JON W. DUDAS

Director of the United States Patent and Trademark Office